

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

**Masking Private Billing Data By Assigning Other  
Billing Data To Use In Commerce With Businesses**

Inventor(s): **Christopher Phillips  
Eric Engstrom**

Prepared by:

**BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP  
12400 Wilshire Boulevard, 7th Floor  
Los Angeles, California 90025  
(503) 684-6200**

**Express Mail Lab I No. EL414991054US**

## 5

holding themselves available to interact using standard protocols such as Hypertext Transfer Protocol (HTTP), and programming languages or environments such as Hypertext Transfer Protocol HTML, XML, Java, JavaScript, Java Beans, ActiveX, Visual Basic, or the like.

- 5 To make a purchase via a web site, a customer executes a "browser," such as the Internet Explorer, Netscape Navigator, or other network aware application program that is configured to communicate with a business' web site. The customer locates a particular product, and proceeds to a "check out" web page (or equivalent) to process a purchase transaction. At this point, the
- 10 customer must enter credit card data and other data sufficient to identify the customer and allow purchase of goods to occur.

Historically, thieves have attempted to monitor such online transactions so as to steal consumer data to allow engaging in subsequent fraudulent transactions. Such monitoring is possible due to the inherently insecure nature

15 of the Internet communication protocol. Internet communication follows the Transmission Control Protocol/Internet Protocol (TCP/IP), where data is broken into small packets that are individually sent to a recipient, received by the recipient and then re-assembled into the original data.

- Unfortunately, anyone with access to a network has the ability to "snoop"
- 20 network traffic on that network. Thus, anyone capable of monitoring some portion of the communication path between the customer and business is then able to monitor the purchase transaction. To overcome this security problem, various protocols, e.g., IP Security (IPSEC), Secure Sockets Layer (SSL),

Secure HTTP (S-HTTP) have emerged to allow a business and a customer to securely communicate.

Although the data packets can still be snooped, their contents are now encrypted and unusable. Thus, thieves have recently begun to attack, or "hack," the online commerce sites so as to steal consumer data stored within databases maintained by the business. Since private consumer data, such as credit card information, once received by a business, is reassembled and decrypted by the business, the data is available for theft.

Thus, what is needed is an environment which provides consumers with the ability to engage in online transactions in a more secure manner.

### **SUMMARY**

Apparatuses and methods registering a user with multiple businesses, where each business is given billing data, such as credit card data, that is unique to that business. Apparatuses, such as computing devices, and consumer electronic devices such as a telephone, communicate with a billing service so that billing data can be generated for particular businesses and used in commercial transactions with the business. Such communication and generation may be in advance of a purchase, or generated in real-time during a purchase.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 illustrates a client in communication with a network.

FIG. 2 is a flow chart according to one embodiment of the invention, illustrating a client registering with a business for purchasing a good.

FIG. 3 is a flowchart according to one embodiment of the invention, in which a client purchases a good using billing data provided in advance by a  
5 billing service.

FIG. 4 is a flowchart according to one embodiment of the invention, in which a client purchases a good using billing data provided in real-time by a billing service.

FIG. 5 illustrates one embodiment of a suitable computing environment in  
10 which certain aspects of the illustrated invention may be implemented.

### **DETAILED DESCRIPTION**

In various embodiments of the invention, a customer is able to establish accounts with web sites without revealing private billing information such as  
15 credit card numbers, advance debit arrangements, invoice arrangements, etc. to a web site / business from whom the customer purchases goods.

FIG. 1 illustrates a client **100** in communication with a network **104**. Also attached to the network are multiple servers **102** (business web sites), such as  
20 those provided by e-commerce sites, online retailers, or other businesses seeking to engage in commerce with by way of networked customers.

It is assumed the client comprises a computing device, such as a personal computer, which operates on behalf of a user (the purchaser of the good). In

alternate embodiments, the client may be incorporated into an electronic card, a telephone (FIG. 6), a personal digital assistant (PDA), a portable audio device, a portable audiovisual device, a cellular telephone, a key-chain dongle, or within an automobile or other transportation device.

5           It is further assumed that each of the network locations to which a client may communicate provide a "web site" for engaging in commercial transactions, and will collectively be referred to as "businesses." For the purposes of this description, the phrase "web site" is intended to be a general reference to a network "presence" maintained by a business as well a logical presence  
10       maintained on behalf of a business.

          The clients **100** and businesses **102** are in communication, through the network **104**, with a billing service **106**. The billing service is configured to allow clients **100** to reduce the risk of disclosing billing data, such as personal credit card numbers, debit card numbers, bank account numbers, and the like, to  
15       businesses **102**. In one embodiment, the billing service facilitates commercial transactions by generating substitute billing data that the client **100** can use when engaging in commercial transactions with businesses **102**. The phrase "substitute billing data" refers to valid billing data that is owned and/or controlled by the billing service **106**, where billing data is temporarily or permanently  
20       distributed to clients **100** to replace personal and/or private billing data of the client.

          Also in communication with the client **100** and businesses **102** by way of the network **104**, is an encryption server **108**. The encryption server can be used

to provide encryption keys to a client **100** and business **102** to allow them to engage in secure communications. In one embodiment, the encryption server **108** is used to engage in conventional public key encryption systems, where the encryption server provides directory assistance services, allowing clients **100** and  
5 businesses **102** to retrieve public encryption keys.

In one embodiment, public key encryption services are used in addition to encryption services already available to a client (e.g., such as those available within a web browser or other communication program used by the client **100**). In an alternate embodiment, already available encryption services, such as those  
10 provided by a web browser, are used to securely communicate with the encryption server **108** to obtain encryption keys for opening a secure communication channel between the client **100** and business **102**.

This allows weaker security afforded by the client communication environment, e.g., a 40 bit or other short key system, to be used to communicate  
15 with the encryption server **108** to obtain more secure (e.g., longer) encryption keys. In this alternate embodiment, the built in security can also be used to transfer non-public key based cryptosystem keys, such as single use session keys, to the client **100** and business **102** for engaging in commerce.

Associated with clients **100** are local storage, such as a database **110**,  
20 that can store billing data and encryption data for use during transactions with a business **102**. In one embodiment, records **112** within the database **110** are keyed on a business **102** identity reference. A business identity can be tracked by way of business name, unique identifier for the business (e.g., a tax ID or

other assigned/selected identifier), uniform resource locator (URL), TCP/IP "dot quad" network address (e.g., 10.1.2.3) used to access the business **102** over the network **104**, or a combination of these and/or other references.

As illustrated, the client local storage containing the database **110** is  
5 integral to a client **100**, such as within local mass storage device(s). However, it will be appreciated that the database may be contained within a separate computing device (not shown) associated with the client **100**, or maintained by or in conjunction with the billing service **106** or encryption server **108**. For example, the billing service **106** or encryption server **108** may be used to store backup  
10 copies of billing data.

FIG. 2 is a flow chart according to one embodiment of the invention, illustrating a client **100** registering with a business **102** for purchasing a good (e.g., a physical or electronic item) from the business.

15 The first illustrated operation is the user initializing **200** the computing device. It is assumed that initialization includes all steps required to boot, wake from an idle state, or otherwise start the computing device and configure it for purchasing activity. Assume that the computing device is a handheld ("palmtop") personal computer executing the Microsoft Windows operating system. After  
20 initialization, the user loads **202** a communication program through which to engage in the purchasing activity.

It will be appreciated that a number of environments may be used to implement the communication program. For example, a dedicated / custom



application program may be designed to access businesses over a network. Alternatively, the communication program can be built using communication features provided by Internet web browser products, such as Microsoft Internet Explorer, Netscape Navigator, or Opera.

5 In this latter environment, the communication program may be implemented in one of, or a combination of, Java, JavaScript, JavaBeans, ActiveX, Visual Basic, HTML, DHTML, or other Internet related programming environments. It is assumed herein the communication program is based on an Internet browser, and that traditional Internet related communication protocols  
10 (e.g., TCP/IP, HTML, etc.) are used to communicate with businesses over the Internet. As discussed with respect to FIG. 1, each business provides a web address to which a client can connect to engage in purchase transactions.

After communication program initialization, the computing device is used to register **204** the user with a first web site maintained by a first business. Note,  
15 however, that even though the illustrated embodiment requires registration, it will be appreciated that in other embodiments, such registration need not occur first, or at all. To register, the computing device contacts **206** the first web site. In response the web site sends an acknowledgement **208**. Since an Internet browser is assumed in use, the contact is by way of directing the browser to an  
20 appropriate receiving port monitored by a web server of the first business. It is assumed that port 80, the traditional Internet communication port, is used for communication. In the web browser context, acknowledgement can be

determined by receiving a "home page" or start page from the first business' web server.

If **210** no acknowledgement is received, then a registration error has occurred and processing of this registration halts **212**; in one embodiment, processing continues on (not shown) with registration attempts with other businesses. If acknowledgement is received, then the client **100** tells the business **102** it is interested in registering with the business **102**.

In one embodiment, the registration process is automated, where the business web server is configured to receive a registration command from the client, and in response the business web server sends the client registration forms to complete. For example, in response to the registration command, an HTML form (or equivalent structure) containing fields for the user's name, address, telephone number, and billing data, such as credit or debit card numbers, invoicing preferences, etc., is sent **214** to the client. This form (or equivalent structure) is completed **216** and returned **218** to the business. In response, the business **102** processes the returned data and registers **220** the client with the billing data returned **218** to the business web server.

Completion of the form can be automated, through automated parsing of the form to identify various fields to fill out. In one embodiment, the extensible markup language (XML) is used to encode forms with semantic meaning to facilitate automatic interpreting and completing of a form. In an alternate embodiment, the user is allowed to review and complete a form with data known to the user, or the user can be provided with an opportunity to review and change

a form completed by the computing device. In another embodiment, a special communication port, analogous to browser port 80, is used to send and receive registration data.

It will be appreciated that even though the above description assumes  
5 registration of a user with businesses, such registration is not required in order to obtain billing data to present to such businesses.

FIG. 3 is a flowchart according to one embodiment of the invention, in which a client **100** purchases a good using billing data provided in advance by a  
10 billing service **106**. This figure concerns the logical data flow for obtaining billing data used by a client **100** in purchasing a good from a business **102**.

As discussed above, there are intrinsic security issues within networks, such as the Internet or home/office local area networks (LANs), when more than just the parties to a conversation may "snoop" data passing on the network so as  
15 to discover secrets (e.g., credit card data or other sensitive data) disclosed during the conversation. In addition to attempts to securely encrypt the data transfers themselves, as will be discussed below, client provided billing data can be customized so as to reduce risk of theft and/or fraudulent use.

A first operation is to contact **302** the billing service. In response, the  
20 billing service asks **304** for the business **102** with which the customer seeks to interact. As discussed above, a variety of different information can be provided to identify the business. For simplicity, it is assumed that the business name is used to identify the business **102**. The business name is provided **306** to the

billing service **106**. In response the billing service generates **308** billing data that can be used by the client in future transactions between the client and the identified business. The correspondence between billing data and business is tracked by the client **100** and/or it is tracked by the billing service **106**.

5           Once the billing data is known, the client **100** can then contact **310** a business and decide **312** on a good to purchase. In response to a purchase decision, the business sends **314** a payment request to the client to arrange for receiving payment for the good. However, unbeknownst to the business **102**, in response to the payment request, instead of sending personal credit card  
10       information, or other payment data, the client **100** instead sends **316** the business the billing data created in advance by the billing service for the business **102**.

          In one embodiment, the billing service obtains the billing data to distribute to clients by entering into agreements with banking institutions (or equivalent).

15       The billing service is provided a large number different billing data, e.g., credit card numbers, debit card numbers, etc., and the billing service may also set up internal invoice accounts and the like. These different billing data are provided to a client **100** when the client registers with the billing service the client's intent to purchase from a business **102**.

20       In one embodiment, billing data presented to a client **100** is uniquely associated with the particular business **102** the client **100** intends to purchase from. Charges made against the billing data are received **318** by the billing service in due course through standard financial institutions such as banks,

savings and loans, investment houses, and the like. These charges are verified  
320 for validity.

In one embodiment, the client informs the billing service of the items  
purchased (or possibly just item categories) so that the billing service may audit a  
5 particular charge to ensure only expected purchases appear on the charge. In  
one embodiment, the client informs the billing service of billing data that is  
provided to businesses so as to facilitate verification. For example, the origin of  
a charge can be compared against the business associated with the billing data.

In this embodiment, if 322 the charge origin fails to match the business  
10 expected to be making the charge, then the charge may be fraudulent.  
Consequently, the charge is contested 324 so as to allow the client to investigate  
the validity of the charge before being billed for the charge. However, if 322 the  
expected business matches the charge origin, then the client is billed for the  
purchase amount paid by the billing service. Note that the client may be billed in  
15 a manner entirely different from the payment system required/used by the  
business 102.

For example, the client may have arranged to have purchases  
automatically deducted from a bank account, while the billing service 106 is  
responsible for honoring a charge made by the business against credit card data  
20 provided by the client 100. Alternatively, the client may have arranged payment  
such that the billing service performs a direct wire transfer from a client's bank  
account directly into a receivables account of the business 102.

By associating a particular business with billing data, it is possible to account for a thief stealing apparently valid billing data from a business' Internet web server, and then attempting to engage in fraudulent activity. In addition to contesting **324** improper charges, the billing service can be configured to retire  
5 billing data that has been compromised.

FIG. 4 is a flowchart according to one embodiment of the invention, in which a client **100** purchases a good using billing data provided in real-time by a billing service **106**. It will be appreciated that even though FIGS. 3 and 4 are  
10 presented separately, a single client may use both real-time generated billing data, and advance-obtained billing data, depending on the business.

After contacting **400** a business **102** from which a purchase is to be made, the client **100** user decides **402** on the purchase; this decision is transmitted to the business. It will be appreciated that this decision-making process may  
15 include the user reviewing various offerings of the business **102** (e.g., "surfing" the business web site), as well as directly connecting to a particular uniform resource location (URL) for purchasing a product (a purchase link may be known in advance).

In response to the purchase decision, the business **102** sends **404** a  
20 payment request to the client. In response, analogous to that described above for FIG. 3, the client contacts **302** the billing service **106**, provides **306** the business name to the service, and receives in real time billing data generated **308** by the billing service for the business **102**. In one embodiment, the billing

data presented to the client **100** is uniquely associated with the particular business **102** the client **100** is purchasing from.

As with FIG. 3, unbeknownst to the business **102**, in response to the payment request **404**, instead of sending personal billing information of the user,  
5 the real time generated billing data is instead sent **406** to the business.

Charges made against the billing data are received **408** by the billing service. As with FIG. 3, these charges are verified **410** for validity. If **412** the charges appear invalid/fraudulent, the charge may be automatically contested **324** or other action taken, such as highlighting the transaction to the user to allow  
10 review of the validity of the charge.

If **412** the charge is valid, then the client is billed for the purchase amount paid by the billing service. Note that the client may be billed in a manner entirely different from the payment system required/used by the business **102**. In one embodiment, highlighting occurs within the bill sent to the user to accentuate  
15 invalid or possibly invalid charges. Highlighting can be by a variety of different methods, such as printing an offending charge in a bold typeface, in a larger type size, in a different font from the rest of the bill, in a different color, in a different section of a bill which organizes suspect charges in a single region, or through a combination of these or other highlighting techniques.

20 In one embodiment, the billing service **106** tracks expiration dates for charges made by the user. That is, if a charge is received against a credit card number provided to a client **100** for purchasing from a business **102**, there may be a timeout period, such as 60 days, in which a charge must be contested if

such charge is to be ever contested. In such circumstances, the highlighting may include prioritization of listed charges according to expiration of contest periods. In another embodiment, a separate bill section is provided for contestable charges expiring within a certain amount of time, such as two weeks.

5           In one embodiment, the client can elect to be billed electronically, in addition to or in lieu of receiving a physical bill printed on paper. Electronic billing can be by way of E-mailing or otherwise electronically transferring bill data to the client. Alternatively, bills can be maintained by the billing service 106, such as through personalized web pages to which a client can log in and review charges.

10          In one embodiment, the personalize web pages include buttons or other controls to allow disputing charges. In one embodiment, single-click buttons are provided with listed charges, where a single click of the button institutes a dispute process to cause the selected charge to be reviewed for fraud.

15           FIG. 5 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which certain aspects of the illustrated invention may be implemented. The invention may be described by reference to different high-level program modules and/or low-level hardware contexts. Those skilled in the art will realize that program module references can  
20          be interchanged with low-level hardware instructions.

Program modules include procedures, functions, programs, components, data structures, and the like, that perform particular tasks or implement particular abstract data types. The modules may be incorporated into single and multi-



5

10

15

20

embodiments, assuming computing device 502 is a client seeking to purchase goods, then remote devices 516, 518 may be a billing service 516 providing substitute billing data to the user for purchasing goods from a business 518.

It will be appreciated that remote computing devices 516, 518 may be configured like computing device 502, and therefore include many or all of the elements discussed for computing device 502. It should also be appreciated that computing devices 502, 516, 518 may be embodied within a single device, or separate communicatively-coupled components, and include routers, bridges, peer devices, web servers, and application programs utilizing network application protocols such as HTTP, File Transfer Protocol (FTP), Gopher, Wide Area Information Server (WAIS), and the like.

Having described and illustrated the principles of the invention with reference to illustrated embodiments, it will be recognized that the illustrated embodiments can be modified in arrangement and detail without departing from such principles.

And, even though the foregoing discussion has focused on particular embodiments, it is understood that other configurations are contemplated. In particular, even though expressions such as "in one embodiment," "in another embodiment," and the like are used herein, these phrases are meant to generally reference embodiment possibilities, and are not intended to limit the invention to particular embodiment configurations.

As used herein, these terms may reference the same or different embodiments, and unless expressly indicated otherwise, are combinable into

other embodiments. Consequently, in view of the wide variety of permutations to the above-described embodiments, the detailed description is intended to be illustrative only, and should not be taken as limiting the scope of the invention.

What is claimed as the invention, therefore, is all such modifications as may

5 come within the scope and spirit of the following claims and equivalents thereto.

0955303-04000